



DoD 5240 1-R

**DEPARTMENT OF DEFENSE**

**PROCEDURES GOVERNING THE  
ACTIVITIES OF  
DOD INTELLIGENCE COMPONENTS  
THAT AFFECT UNITED STATES PERSONS**

**DECEMBER 1982**

**UNDER SECRETARY OF DEFENSE FOR POLICY**

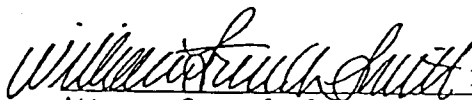
FOREWORD

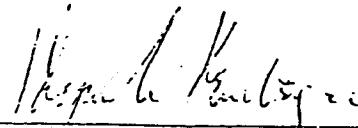
This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect United States persons. It implements DoD Directive 5240.1, and replaces the November 30, 1979 version of DoD Regulation 5240.1-R. It is applicable to all DoD intelligence components.

Executive Order 12333, "United States Intelligence Activities," stipulates that certain activities of intelligence components that affect U.S. persons be governed by procedures issued by the agency head and approved by the Attorney General. Specifically, procedures 1 through 10, as well as Appendix A, herein, require approval by the Attorney General. Procedures 11 through 15, while not requiring approval by the Attorney General, contain further guidance to DoD Components in implementing Executive Order 12333 as well as Executive Order 12334, "President's Intelligence Oversight Board".

Accordingly, by this memorandum, these procedures are approved for use within the Department of Defense. Heads of DoD components shall issue such implementing instructions as may be necessary for the conduct of authorized functions in a manner consistent with the procedures set forth herein.

This regulation is effective immediately.

  
10/4/82  
Attorney General of the  
United States

  
12/7/82  
Secretary of Defense

## TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	2
TABLE OF CONTENTS	3
REFERENCES	6
DEFINITIONS	7
CHAPTER 1 - PROCEDURE 1. GENERAL PROVISIONS	13
C1.1. APPLICABILITY AND SCOPE	13
C1.2. SCOPE	13
C1.3. INTERPRETATION	14
C1.4. EXCEPTIONS TO POLICY	14
C1.5. AMENDMENT	14
CHAPTER 2 - PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS	15
C2.1. APPLICABILITY AND SCOPE	15
C2.2. EXPLANATION OF UNDEFINED TERMS	15
C2.3. TYPES OF INFORMATION THAT MAY BE COLLECTED ABOUT UNITED STATES PERSONS	16
C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS	18
C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES	18
CHAPTER 3 - PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS	20
C3.1. APPLICABILITY	20
C3.2. EXPLANATION OF UNDEFINED TERMS	20
C3.3. CRITERIA FOR RETENTION	20
C3.4. ACCESS AND RETENTION	21
CHAPTER 4 - PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS	22
C4.1. APPLICABILITY AND SCOPE	22
C4.2. CRITERIA FOR DISSEMINATION	22
C4.3. OTHER DISSEMINATION	23

TABLE OF CONTENTS, continued

CHAPTER 5 - PROCEDURE 5. ELECTRONIC SURVEILLANCE	<u>Page</u> 24
C5.1. PART 1. ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES	24
C5.2. PART 2. ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES	25
C5.3. PART 3. SIGNALS INTELLIGENCE ACTIVITIES	28
C5.4. PART 4. TECHNICAL SURVEILLANCE COUNTERMEASURES	31
C5.5. PART 5. DEVELOPING, TESTING AND CALIBRATION OF ELECTRONIC EQUIPMENT	32
C5.6. PART 6. TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT	34
C5.7. PART 7. CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS	36
CHAPTER 6 - PROCEDURE 6. CONCEALED MONITORING	38
C6.1. APPLICABILITY AND SCOPE	38
C6.2. EXPLANATION OF UNDEFINED TERMS	38
C6.3. PROCEDURES	39
CHAPTER 7 - PROCEDURE 7. PHYSICAL SEARCHES	41
C7.1. APPLICABILITY AND SCOPE	41
C7.2. EXPLANATION OF UNDEFINED TERMS	41
C7.3. PROCEDURES	41
CHAPTER 8 - PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL	45
C8.1. APPLICABILITY	45
C8.2. EXPLANATION OF UNDEFINED TERMS	45
C8.3. PROCEDURES	46
CHAPTER 9 - PROCEDURE 9. PHYSICAL SURVEILLANCE	47
C9.1. APPLICABILITY	47
C9.2. EXPLANATION OF UNDEFINED TERMS	47
C9.3. PROCEDURES	47

## TABLE OF CONTENTS, continued

	<u>Page</u>
CHAPTER 10 - PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS	49
C10.1. APPLICABILITY	49
C10.2. EXPLANATION OF UNDEFINED TERMS	49
C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION	50
C10.4. DISCLOSURE REQUIREMENT	53
CHAPTER 11 - PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES	54
C11.1. APPLICABILITY	54
C11.2. PROCEDURES	54
C11.3. EFFECT OF NONCOMPLIANCE	55
CHAPTER 12 - PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES	56
C12.1. APPLICABILITY	56
C12.2. PROCEDURES	56
CHAPTER 13 - PROCEDURE 13. EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES	58
C13.1. APPLICABILITY	58
C13.2. EXPLANATION OF UNDEFINED TERMS	58
C13.3. PROCEDURES	58
CHAPTER 14 - PROCEDURE 14. EMPLOYEE CONDUCT	60
C14.1. APPLICABILITY	60
C14.2. PROCEDURES	60
CHAPTER 15 - PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE ACTIVITIES	62
C15.1. APPLICABILITY	62
C15.2. EXPLANATION OF UNDEFINED TERMS	62
C15.3. PROCEDURES	62

## REFERENCES

- (a) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (b) Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978"
- (c) DoD Directive 5200.29, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," February 12, 1975
- (d) Chapters 105 and 119 of title 18, United States Code
- (e) Public Law 73-416, "Communications Act of 1934," Section 605
- (f) Sections 801-840 of title 10, United States Code, "Uniform Code of Military Justice"
- (g) Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979
- (h) Executive Order 12198, "Prescribing Amendments to the Manual for Courts-Martial, United States, 1969," March 12, 1980
- (i) DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," March 22, 1982
- (j) DoD Directive 5000.11, "Data Elements and Data Codes Standardization Program," December 7, 1964
- (k) DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976

## DL1. DEFINITIONS

DL1.1.1. Administrative Purposes. Information is collected for "administrative purposes" when it is necessary for the administration of the component concerned, but is not collected directly in performance of the intelligence activities assigned such component. Examples include information relating to the past performance of potential contractors; information to enable such components to discharge their public affairs and legislative duties, including the maintenance of correspondence files; the maintenance of employee personnel and training records; and training materials or documents produced at training facilities.

DL1.1.2. Available Publicly. Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

DL1.1.3. Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such telecommunications.

DL1.1.4. Consent. The agreement by a person or organization to permit DoD intelligence components to take particular actions that affect the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure. Consent may be implied if adequate notice is provided that a particular action (such as entering a building) carries with it the presumption of consent to an accompanying action (such as search of briefcases). (Questions regarding what is adequate notice in particular circumstances should be referred to the legal office responsible for advising the DoD intelligence component concerned.)

DL1.1.5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

DL1.1.6. Counterintelligence Investigation. Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

DL1.1.7. DoD Component. Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

DL1.1.8. DoD Intelligence Components. Include the following organizations:

DL1.1.8.1. The National Security Agency/Central Security Service.

DL1.1.8.2. The Defense Intelligence Agency.

DL1.1.8.3. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

DL1.1.8.4. The Assistant Chief of Staff for Intelligence, Army General Staff.

DL1.1.8.5. The Office of Naval Intelligence.

DL1.1.8.6. The Assistant Chief of Staff, Intelligence, U. S. Air Force.

DL1.1.8.7. The Army Intelligence and Security Command.

DL1.1.8.8. The Naval Intelligence Command.

DL1.1.8.9. The Naval Security Group Command.

DL1.1.8.10. The Director of Intelligence, U.S. Marine Corps.

DL1.1.8.11. The Air Force Intelligence Service.

DL1.1.8.12. The Electronic Security Command, U.S. Air Force.

DL1.1.8.13. The counterintelligence elements of the Naval Investigative Service.

DL1.1.8.14. The counterintelligence elements of the Air Force Office of Special Investigations.



DL1.1.8.15. The 650th Military Intelligence Group, SHAPE.

DL1.1.8.16. Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

DL1.1.9. Electronic Surveillance. Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)

DL1.1.10. Employee. A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency.

DL1.1.11. Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

DL1.1.12. Foreign Power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

DL1.1.13. Intelligence Activities. Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a)).

DL1.1.14. Intelligence Community and an Agency of Or Within the Intelligence Community. Refers to the following organizations:

DL1.1.14.1. The Central Intelligence Agency (CIA).

DL1.1.14.2. The National Security Agency (NSA).

DL1.1.14.3. The Defense Intelligence Agency (DIA).

DL1.1.14.4. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

DL1.1.14.5. The Bureau of Intelligence and Research of the Department of State.

DL1.1.14.6. The intelligence elements of the Army, the Navy, the Air Force and the Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.

DL1.1.14.7. The staff elements of the Office of the Director of Central Intelligence.

DL1.1.15. International Narcotics Activities. Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with Sections 811 and 812 of title 21, United States Code.

DL1.1.16. International Terrorist Activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

DL1.1.17. Lawful Investigation. An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction; if it is conducted by a DoD Component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security); and if the investigation is conducted in accordance with applicable law and policy, including E.O. 12333 and this Regulation.

DL1.1.18. Personnel Security. Measures designed to insure that persons employed, or being considered for employment, in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

DL1.1.19. Personnel Security Investigation:

DL1.1.19.1. An inquiry into the activities of a person granted access to intelligence or other classified information; or a person who is being considered for access to intelligence or other classified information, including persons who are granted or may be granted access to facilities of DoD intelligence components; or a person to be assigned or retained in a position with sensitive duties. The investigation is designed to develop information pertaining to the suitability, eligibility, and trustworthiness of the individual with respect to loyalty, character, emotional stability and reliability.

DL1.1.19.2. Inquiries and other activities directed against DoD employees or members of a Military Service to determine the facts of possible voluntary or involuntary compromise of classified information by them.

DL1.1.19.3. The collection of information about or from military personnel in the course of tactical training exercises for security training purposes.

DL1.1.20. Physical Security. The physical measures taken to prevent unauthorized access to, and prevent the damage or loss of, equipment, facilities, materiel and documents; and measures undertaken to protect DoD personnel from physical threats to their safety.

DL1.1.21. Physical Security Investigation. All inquiries, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and all inquiries and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property.

DL1.1.22. Reasonable Belief. A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not.

DL1.1.23. Signals Intelligence. A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

DL1.1.24. United States. When used to describe a place, the term shall include the territories under the sovereignty of the United States.

DL1.1.25. United States Person

DL1.1.25.1. The term "United States person" means:

DL1.1.25.1.1. A United States citizen;

DL1.1.25.1.2. An alien known by the DoD intelligence component concerned to be a permanent resident alien;

DL1.1.25.1.3. An unincorporated association substantially composed of United States citizens or permanent resident aliens;

DL1.1.25.1.4. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.

DL1.1.25.2. A person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained.

DL1.1.25.3. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.

## C1. CHAPTER 1

### PROCEDURE 1. GENERAL PROVISIONS

#### C1.1. APPLICABILITY AND SCOPE

C1.1.1. These procedures apply only to "DoD intelligence components," as defined in the Definitions Section. Procedures 2 through 4 provide the sole authority by which such components may collect, retain and disseminate information concerning United States persons. Procedures 5 through 10 set forth applicable guidance with respect to the use of certain collection techniques to obtain information for foreign intelligence and counterintelligence purposes. Authority to employ such techniques shall be limited to that necessary to perform functions assigned the DoD intelligence component concerned. Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities.

C1.1.2. The functions of DoD intelligence components not specifically addressed herein shall be carried out in accordance with applicable policy and procedure.

C1.1.3. These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcement procedures.

C1.1.4. DoD intelligence components shall not request any person or entity to undertake any activity forbidden by Executive Order 12333 (reference (a)).

#### C1.2. PURPOSE

The purpose of these procedures is to enable DoD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

### C1.3. INTERPRETATION

C1.3.1. These procedures shall be interpreted in accordance with their stated purpose.

C1.3.2. All defined terms appear in the Definitions Section. Additional terms, not otherwise defined, are explained in the text of each procedure, as appropriate.

C1.3.3. All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned. Questions that cannot be resolved in this manner shall be referred to the General Counsel of the Military Department concerned, or, as appropriate, the General Counsel of the Department of Defense for resolution.

### C1.4. EXCEPTIONS TO POLICY

Requests for exception to the policies and procedures established herein shall be made in writing to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense and, if required, the Attorney General for any such exception.

### C1.5. AMENDMENT

Requests for amendment of these procedures shall be made to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense, and, if required, the Attorney General, for any such amendment.

## C2. CHAPTER 2

### PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

#### C2.1. APPLICABILITY AND SCOPE

This procedure specifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information. Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques.

#### C2.2. EXPLANATION OF UNDEFINED TERMS

C2.2.1. Collection. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

C2.2.2. Cooperating sources means persons or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information, at the request of such components or on their own initiative. These include Government Agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments.

C2.2.3. Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization, or person.

C2.2.4. Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that he is providing such information to the Department of Defense or a component thereof.

### C2.3. TYPES OF INFORMATION THAT MAY BE COLLECTED ABOUT UNITED STATES PERSONS

Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:

C2.3.1. Information Obtained With Consent. Information may be collected about a United States person who consents to such collection.

C2.3.2. Publicly Available Information. Information may be collected about a United States person if it is publicly available.

C2.3.3. Foreign Intelligence. Subject to the special limitation contained in section C2.5., below, information may be collected about a United States person if the information constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are:

C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;

C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;

C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;

C2.3.3.4. Persons who are reasonably believed to be prisoners of war; missing in action; or are the targets, the hostages, or victims of international terrorist organizations; or

C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

C2.3.4. Counterintelligence. Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:

C2.3.4.1. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.



C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

C2.3.5. Potential Sources of Assistance to Intelligence Activities. Information may be collected about United States persons reasonably believed to be potential sources of intelligence, or potential sources of assistance to intelligence activities, for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

C2.3.6. Protection of Intelligence Sources and Methods. Information may be collected about a United States person who has access to, had access to, or is otherwise in possession of, information that reveals foreign intelligence and counterintelligence sources or methods, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information; provided that within the United States, intentional collection of such information shall be limited to persons who are:

C2.3.6.1. Present and former DoD employees;

C2.3.6.2. Present or former employees of a present or former DoD contractor; and

C2.3.6.3. Applicants for employment at the Department of Defense or at a contractor of the Department of Defense.

C2.3.7. Physical Security. Information may be collected about a United States person who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors. Information may also be collected in the course of a lawful physical security investigation.

C2.3.8. Personnel Security. Information may be collected about a United States person that arises out of a lawful personnel security investigation.

C2.3.9. Communications Security. Information may be collected about a United States person that arises out of a lawful communications security investigation.

C2.3.10. Narcotics. Information may be collected about a United States person who is reasonably believed to be engaged in international narcotics activities.

C2.3.11. Threats to Safety. Information may be collected about a United States person when the information is needed to protect the safety of any person or

organization, including those who are targets, victims, or hostages of international terrorist organizations.

C2.3.12. Overhead Reconnaissance. Information may be collected from overhead reconnaissance not directed at specific United States persons.

C2.3.13. Administrative Purposes. Information may be collected about a United States person that is necessary for administrative purposes.

#### C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS

C2.4.1. Means of Collection. DoD intelligence components are authorized to collect information about United States persons by any lawful means, provided that all such collection activities shall be carried out in accordance with E.O. 12333 (reference (a)), and this Regulation, as appropriate.

C2.4.2. Least Intrusive Means. The collection of information about United States persons shall be accomplished by the least intrusive means. In general, this means the following:

C2.4.2.1. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned;

C2.4.2.2. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources;

C2.4.2.3. If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General; then

C2.4.2.4. If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought.

#### C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES

Within the United States, foreign intelligence concerning United States persons may be collected only by overt means unless all the following conditions are met:

C2.5.1. The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any United States person;

C2.5.2. Such foreign intelligence cannot be reasonably obtained by overt means;

C2.5.3. The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI); and

C2.5.4. The use of other than overt means has been approved in writing by the head of the DoD intelligence component concerned, or his single designee, as being consistent with these procedures. A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy).

### C3. CHAPTER 3

#### PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

##### C3.1. APPLICABILITY

This procedure governs the kinds of information about United States persons that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns. It does not apply when the information in question is retained solely for administrative purposes or is required by law to be maintained.

##### C3.2. EXPLANATION OF UNDEFINED TERMS

The term "retention," as used in this procedure, refers only to the maintenance of information about United States persons that can be retrieved by reference to the person's name or other identifying data.

##### C3.3. CRITERIA FOR RETENTION

C3.3.1. Retention of Information Collected Under Procedure 2. Information about United States persons may be retained if it was collected pursuant to Procedure 2.

C3.3.2. Retention of Information Acquired Incidentally. Information about United States persons collected incidentally to authorized collection may be retained if:

C3.3.2.1. Such information could have been collected intentionally under Procedure 2;

C3.3.2.2. Such information is necessary to understand or assess foreign intelligence or counterintelligence;

C3.3.2.3. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation; or

C3.3.2.4. Such information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

C3.3.3. Retention of Information Relating to Functions of Other DoD Components or non-DoD Agencies. Information about United States persons that pertains solely to the functions of other DoD Components or Agencies outside the Department of Defense shall be retained only as necessary to transmit or deliver such information to the appropriate recipients.

C3.3.4. Temporary Retention. Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures.

C3.3.5. Retention of Other Information. Information about United States persons other than that covered by paragraphs C3.3.1. through C3.3.4., above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

#### C3.4. ACCESS AND RETENTION

C3.4.1. Controls On Access to Retained Information. Access within a DoD intelligence component to information about United States persons retained pursuant to this procedure shall be limited to those with a need to know.

C3.4.2. Duration of Retention. Disposition of information about United States Persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained.

C3.4.3. Information Acquired Prior to Effective Date. Information acquired prior to the effective date of this procedure may be retained by DoD intelligence components without being screened for compliance with this procedure or Executive Order 12333 (reference (a)), so long as retention was in compliance with applicable law and previous Executive orders.

## C4. CHAPTER 4

### PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

#### C4.1. APPLICABILITY AND SCOPE

This procedure governs the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information. It does not apply to information collected solely for administrative purposes; or disseminated pursuant to law; or pursuant to a court order that otherwise imposes controls upon such dissemination.

#### C4.2. CRITERIA FOR DISSEMINATION

Except as provided in section C4.3., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

C4.2.1. The information was collected or retained or both under Procedures 2 and 3;

C4.2.2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:

C4.2.2.1. An employee of the Department of Defense, or an employee of a contractor of the Department of Defense, and has a need for such information in the course of his or her official duties;

C4.2.2.2. A law enforcement entity of Federal, State, or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce;

C4.2.2.3. An Agency within the intelligence community; provided that within the intelligence community, information other than information derived from signals intelligence, may be disseminated to each appropriate Agency for the purpose of allowing the recipient Agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component;

C4.2.2.4. An Agency of the Federal Government authorized to receive such information in the performance of a lawful governmental function; or

C4.2.2.5. A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

#### C4.3. OTHER DISSEMINATION

Any dissemination that does not conform to the conditions set forth in section C4.2., above, must be approved by the legal office responsible for advising the DoD Component concerned after consultation with the Department of Justice and General Counsel of the Department of Defense. Such approval shall be based on determination that the proposed dissemination complies with applicable laws, Executive orders, and regulations.

## C5. CHAPTER 5

### PROCEDURE 5. ELECTRONIC SURVEILLANCE

#### C5.1. PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.1.1. Applicability. This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1979 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

#### C5.1.2. General Rules

C5.1.2.1. Electronic Surveillance Pursuant to the Foreign Intelligence Surveillance Act. A DoD intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes only pursuant to an order issued by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978 (reference (b)), or pursuant to a certification of the Attorney General issued under the authority of Section 102(a) of the Act.

C5.1.2.2. Authority to Request Electronic Surveillance. Authority to approve the submission of applications or requests for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (reference (b)) shall be limited to the Secretary of Defense, the Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency. Applications for court orders will be made through the Attorney General after prior clearance by the General Counsel, DoD. Requests for Attorney General certification shall be made only after prior clearance by the General Counsel, DoD.

#### C5.1.2.3. Electronic Surveillance In Emergency Situations

C5.1.2.3.1. A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General in accordance with Section 105(e) of reference (b).

C5.1.2.3.2. The head of a DoD intelligence component may request that the DoD General Counsel seek such authority directly from the Attorney General in an emergency, if it is not feasible to submit such request through an official designated in subparagraph C5.1.2.2., above, provided the appropriate official concerned shall be advised of such requests as soon as possible thereafter.



## C5.2. PART 2: ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.2.1. Applicability. This part of Procedure 5 applies to electronic surveillance, as defined in the Definitions Section, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 and the regulation of "signals intelligence activities" under Part 3 so that the intentional interception for foreign intelligence and counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts. In addition, this part governs the use of electronic, mechanical, or other surveillance devices for foreign intelligence and counterintelligence purposes against a United States person abroad in circumstances where such person has a reasonable expectation of privacy. This part does not apply to the electronic surveillance of communications of other than United States persons abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

### C5.2.2. Explanation of Undefined Terms

C5.2.2.1. Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person. Electronic surveillance directed against persons who are not United States persons that results in the incidental acquisition of the communications of a United States person does not thereby become electronic surveillance directed against a United States person.

C5.2.2.2. Electronic surveillance is "outside the United States" if the person against whom the electronic surveillance is directed is physically outside the United States, regardless of the location at which surveillance is conducted. For example, the interception of communications that originate and terminate outside the United States can be conducted from within the United States and still fall under this part rather than Part 1.

C5.2.3. Procedures. Except as provided in paragraph C5.2.5., below, DoD intelligence components may conduct electronic surveillance against a United States person who is outside the United States for foreign intelligence and counterintelligence purposes only if the surveillance is approved by the Attorney General. Requests for

approval will be forwarded to the Attorney General by an official designated in subparagraph C5.2.5.1., below. Each request shall include:

C5.2.3.1. An identification or description of the target.

C5.2.3.2. A statement of the facts supporting a finding that:

C5.2.3.2.1. There is probable cause to believe the target of the electronic surveillance is one of the following:

C5.2.3.2.1.1. A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;

C5.2.3.2.1.2. A person who is an officer or employee of a foreign power;

C5.2.3.2.1.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this paragraph, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C5.2.3.2.1.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C5.2.3.2.1.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

C5.2.3.2.2. The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence.

C5.2.3.2.3. The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be obtained by other less intrusive collection techniques.

C5.2.3.3. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance.

C5.2.3.4. A description of the means by which the electronic surveillance will be effected.

C5.2.3.5. If physical trespass is required to effect the surveillance, a statement of facts supporting a finding that the means involve the least amount of intrusion that will accomplish the objective.

C5.2.3.6. A statement of period of time, not to exceed 90 days, for which the electronic surveillance is required.

C5.2.3.7. A description of the expected dissemination of the product of the surveillance, including a description of the procedures that will govern the retention and dissemination of communications of or concerning United States persons other than those targeted, acquired incidental to such surveillance.

C5.2.4. Electronic Surveillance in Emergency Situations. Notwithstanding paragraph C5.2.3., above, a DoD intelligence component may conduct surveillance directed at a United States person who is outside the United States in emergency situations under the following limitations:

C5.2.4.1. Officials designated in paragraph C5.2.5., below, may authorize electronic surveillance directed at a United States person outside the United States in emergency situations, when securing the prior approval of the Attorney General is not practical because:

C5.2.4.1.1. The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security;

C5.2.4.1.2. A person's life or physical safety is reasonably believed to be in immediate danger; or

C5.2.4.1.3. The physical security of a defense installation or Government property is reasonably believed to be in immediate danger.

C5.2.4.2. Except for actions taken under subparagraph C5.2.4.1.2., above, any official authorizing such emergency surveillance shall find that one of the criteria contained in subparagraph C5.2.3.2.1., above, is met. Such officials shall notify the DoD General Counsel promptly of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results.

C5.2.4.3. The Attorney General shall be notified by the General Counsel, DoD, as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and such other information as may be required to authorize continuation of such surveillance.

C5.2.4.4. Electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

C5.2.5. Officials Authorized to Request and Approve Electronic Surveillance Outside the United States

C5.2.5.1. The following officials may request approval of electronic surveillance outside the United States under paragraph C5.2.3., above, and approve emergency surveillance under paragraph C5.2.4., above:

C5.2.5.1.1. The Secretary and Deputy Secretary of Defense.

C5.2.5.1.2. The Secretaries and Under Secretaries of the Military Departments.

C5.2.5.1.3. The Director and Deputy Director of the National Security Agency/Chief, Central Security Service.

C5.2.5.2. Authorization for emergency electronic surveillance under paragraph C5.2.4., may also be granted by:

C5.2.5.2.1. Any general or flag officer at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered, or

C5.2.5.2.2. The Deputy Director for Operations, National Security Agency.

C5.3. PART3: SIGNALS INTELLIGENCE ACTIVITIES

C5.3.1. Applicability and Scope

C5.3.1.1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection,

retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.

C5.3.1.2. This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the Attorney General. That regulation shall provide that signals intelligence activities that constitute electronic surveillance, as defined in Parts 1, and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the Attorney General.

C5.3.2. Explanation of Undefined Terms

C5.3.2.1. Communications concerning a United States person are those in which the United States person is identified in the communication. A United States person is identified when the person's name, unique title, address or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Monroe Doctrine," is not an identification of a United States person.

C5.3.2.2. Interception means the acquisition by the United States Signals Intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signals.

C5.3.2.3. Military tactical communications means United States and allied military exercise communications within the United States and abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

C5.3.2.4. United States Person. For purposes of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person:

C5.3.2.4.1. A person known to be currently in the United States will be treated as a United States person unless the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.

C5.3.2.4.2. A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.

C5.3.2.4.3. A person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

C5.3.2.4.4. An unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence.

C5.3.2.5. United States Signals Intelligence System means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the Military Services authorized to conduct signals intelligence and such other entities (other than the Federal Bureau of Investigation) as are authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence. FBI activities are governed by procedures promulgated by the Attorney General.

### C5.3.3. Procedures

C5.3.3.1. Foreign Communications. The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure.

C5.3.3.2. Military Tactical Communications. The United States Signals Intelligence System may collect, process, retain, and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure.

C5.3.3.2.1. Collection. Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercises.

C5.3.3.2.2. Retention and Processing. Military tactical communications may be retained and processed without deletion of references to United States persons who are participants in, or are otherwise mentioned in exercise-related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible.

C5.3.3.2.3. Dissemination. Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating in or conducting reviews and critiques of such exercise.

#### C5.4. PART 4: TECHNICAL SURVEILLANCE COUNTERMEASURES

C5.4.1. Applicability and Scope. This part of Procedure 5 applies to the use of electronic equipment to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements Section 105(f)(2) of the Foreign Intelligence Surveillance Act (reference (b)).

C5.4.2. Explanation of Undefined Terms. The term technical surveillance countermeasures refers to activities authorized pursuant to DoD Directive 5200.29 (reference (c)), and, as used in this procedure, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, or for determining the susceptibility of electronic equipment to unlawful electronic surveillance.

C5.4.3. Procedures A DoD intelligence component may use technical surveillance countermeasures that involve the incidental acquisition of the nonpublic communications of United States persons without their consent, provided:

C5.4.3.1. The use of such countermeasures has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken;

C5.4.3.2. The use of such countermeasures is limited in that necessary to determine the existence and capability of such equipment; and

C5.4.3.3. Access to the content of communications acquired during the use of countermeasures is limited to persons involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use. However, if the content is acquired within the United States, only information that is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (d)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated only for these purposes. If acquired outside the United States, information that indicates a violation of Federal law, including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities. A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained.

## C5.5. PART 5: DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENT

C5.5.1. Applicability This part of Procedure 5 applies to developing, testing, or calibrating electronic equipment that can intercept or process communications and non-communications signals. It also includes research and development that needs electronic communications as a signal source.

### C5.5.2. Procedures

#### C5.5.2.1. Signals Authorized for Use

C5.5.2.1.1. The following may be used without restriction:

C5.5.2.1.1.1. Laboratory-generated signals.



C5.5.2.1.1.2. Communications signals with the consent of the communicator.

C5.5.2.1.1.3. Communications in the commercial or public service broadcast bands.

C5.5.2.1.1.4. Communications transmitted between terminals located outside of the United States not used by any known United States person.

C5.5.2.1.1.5. Non-communications signals (including telemetry, and radar).

C5.5.2.1.2. Communications subject to lawful electronic surveillance under the provisions of Parts 1, 2, or 3, of this procedure may be used subject to the minimization procedures applicable to such surveillance.

C5.5.2.1.3. Any of the following may be used subject to the restrictions of subparagraph C5.5.2.2., below.

C5.5.2.1.3.1. Communications over official Government communications circuits with consent from an appropriate official of the controlling agency.

C5.5.2.1.3.2. Communications in the citizens and amateur-radio bands.

C5.5.2.1.4. Other signals may be used only when it is determined that it is not practical to use the signals described above and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. The restrictions of subparagraph C5.5.2.2., below, will apply in such cases. The Attorney General must approve use of signals pursuant to this subsection for the purpose of development, testing, or calibration when the period of use exceeds 90 days. When Attorney General approval is required, the DoD intelligence component shall submit a test proposal to the General Counsel, DoD, or the NSA General Counsel for transmission to the Attorney General for approval. The test proposal shall state the requirement for a period beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity.

C5.5.2.2. Restrictions. For signals described in subparagraphs C5.5.2.1.3. and C5.5.2.1.4., above, the following restrictions apply:

C5.5.2.2.1. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in paragraph C5.5.1., above.

C5.5.2.2.2. No particular United States person shall be targeted intentionally without consent.

C5.5.2.2.3. The content of any communication shall:

C5.5.2.2.3.1. Be retained only when actually needed for the purposes referred to in paragraph C5.5.1., above;

C5.5.2.2.3.2. Be disseminated only to persons conducting the activity; and

C5.5.2.2.3.3. Be destroyed immediately upon completion of the activity.

C5.5.2.2.4. The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes outlined in paragraph C5.5.1., above, or for collection avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment provided such dissemination and use are limited to the purposes outlined in paragraph C5.5.1., or collection avoidance purposes. No content of any communication may be retained or used other than as provided in subparagraph C5.5.2.2.3., above.

## C5.6. PART 6: TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

C5.6.1. Applicability. This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment. It does not apply to the interception of communications with the consent of one of the parties to the communication or to the training of intelligence personnel by non-intelligence components.

### C5.6.2. Procedures

C5.6.2.1. Training Guidance. The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance

equipment shall include guidance concerning the requirements and restrictions of the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and E.O. 12333 (reference (a)), with respect to the unauthorized acquisition and use of the content of communications of United States persons.

#### C5.6.2.2. Training Limitations

C5.6.2.2.1. Except as permitted by paragraph C5.6.2.2.2. and C5.6.2.2.3., below, the use of electronic communications and surveillance equipment for training purposes is permitted, subject to the following limitations:

C5.6.2.2.1.1. To the maximum extent practical, use of such equipment for training purposes shall be directed against communications that are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure.

C5.6.2.2.1.2. The contents of private communications of non-consenting United States persons may not be acquired aurally unless the person is an authorized target of electronic surveillance.

C5.6.2.2.1.3. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

C5.6.2.2.2. Public broadcasts, distress signals, or official U.S. Government communications may be monitored, provided that when Government Agency communications are monitored, the consent of an appropriate official is obtained.

C5.6.2.2.3. Minimal acquisition of information is permitted as required for calibration purposes.

C5.6.2.3. Retention and Dissemination. Information collected during training that involves communications described in subparagraph C5.6.2.2.1.1., above, shall be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance. Information collected during training that does not involve communications described in subparagraph C5.6.2.2.1.1., above, or that is acquired inadvertently, shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This limitation does not apply to distress signals.

## C5.7. PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS

C5.7.1. Applicability and Scope This part of Procedure 5 applies to the conduct of vulnerability surveys and hearability surveys by DoD intelligence components.

### C5.7.2. Explanation of Undefined Terms

C5.7.2.1. The term vulnerability survey refers to the acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.

C5.7.2.2. The term hearability survey refers to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the hearability of reception over time.

### C5.7.3. Procedures

C5.7.3.1. Conduct of Vulnerability Surveys. Nonconsensual surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of transmission facilities of communications common carriers, other private commercial entities, and entities of the federal government, subject of the following limitations:

C5.7.3.1.1. No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee.

C5.7.3.1.2. No transmission may be acquired aurally.

C5.7.3.1.3. No content of any transmission may be acquired by any means.

C5.7.3.1.4. No transmissions may be recorded.

C5.7.3.1.5. No report or log may identify any United States person or entity except to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

C5.7.3.2. Conduct of Hearability Surveys. The Director, National Security Agency, may conduct, or may authorize the conduct by other Agencies, of hearability surveys of telecommunications that are transmitted in the United States.

C5.7.3.2.1. Collection. When practicable, consent will be secured from the owner or user of the facility against which the hearability survey is to be conducted prior to the commencement of the survey.

C5.7.3.2.2. Processing and Storage. Information collected during a hearability survey must be processed and stored as follows:

C5.7.3.2.2.1. The content of communications may not be recorded or included in any report.

C5.7.3.2.2.2. No microwave transmission may be de-multiplexed or demodulated for any purpose.

C5.7.3.2.2.3. No report or log may identify any person or entity except to the extent of identifying the transmission facility that can be intercepted from the intercept site. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the hearability survey has been conducted, the identity of such users may be obtained provided such identities may not be obtained from the contents of the transmissions themselves.

C5.7.3.2.3. Dissemination. Reports may be disseminated only within the U.S. Government. Logs may not be disseminated unless required to verify results contained in reports.

## C6. CHAPTER 6

### PROCEDURE 6. CONCEALED MONITORING

#### C6.1. APPLICABILITY AND SCOPE

C6.1.1. This procedure applies to concealed monitoring only for foreign intelligence and counterintelligence purposes conducted by a DoD intelligence component within the United States or directed against a United States person who is outside the United States where the subject of such monitoring does not have a reasonable expectation of privacy, as explained in section 6.2., below, and no warrant would be required if undertaken for law enforcement purposes.

C6.1.2. Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure.

C6.1.3. Concealed monitoring for foreign intelligence and counterintelligence purposes of a United States person abroad where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance outside the United States" under Part 2 of Procedure 5, and processed pursuant to that procedure.

C6.1.4. Concealed monitoring for foreign intelligence and counterintelligence purposes when the monitoring is a signals intelligence activity shall be conducted pursuant to Part 3 of Procedure 5.

#### C6.2. EXPLANATION OF UNDEFINED TERMS

C6.2.1. Concealed monitoring means targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time.

C6.2.2. Monitoring is within the United States if the monitoring device, or the target of the monitoring, is located within the United States.

C6.2.3. Whether concealed monitoring is to occur where the subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office responsible for advising the DoD intelligence component concerned. Reasonable expectation of privacy is the extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to monitoring by electronic, optical, or mechanical devices. For example, there are ordinarily reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal working conditions. Conversely, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed; however, such a person ordinarily would have an expectation of privacy within his or her residence.

### C6.3. PROCEDURES

C6.3.1. Limitations On Use of Concealed Monitoring. Use of concealed monitoring under circumstances when the subject of such monitoring has no reasonable expectation of privacy is subject to the following limitations:

C6.3.1.1. Within the United States, a DoD intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by the Department of Defense or otherwise in the course of an investigation conducted pursuant to the Agreement Between the Secretary of Defense and the Attorney General (reference (g)).

C6.3.1.2. Outside the United States, such monitoring may be conducted on installations and facilities owned or leased by the Department of Defense. Monitoring outside such facilities shall be conducted after coordination with appropriate host country officials, if such coordination is required by the governing Status of Forces Agreement, and with the Central Intelligence Agency.

C6.3.2. Required Determination. Concealed monitoring conducted under paragraph C6.3.1., requires approval by an official designated in paragraph C6.3.3., below, based on a determination that such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions, and does not constitute electronic surveillance under Parts 1 or 2 of Procedure 5.

C6.3.3. Officials Authorized to Approve Concealed Monitoring. Officials authorized to approve concealed monitoring under this procedure include the Deputy

Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Director, National Security Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Director, Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, U.S. Air Force; the Commanding General, Army Intelligence and Security Command; the Director, Naval Investigative Service; and the Commanding Officer, Air Force Office of Special Investigations.



## C7. CHAPTER 7

### PROCEDURE 7. PHYSICAL SEARCHES

#### C7.1. APPLICABILITY

This procedure applies to nonconsensual physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes. DoD intelligence components may provide assistance to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12.

#### C7.2. EXPLANATION OF UNDEFINED TERMS

Physical search means any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. The term also does not include any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to Parts 1 and 2 of Procedure 5.

#### C7.3. PROCEDURES

##### C7.3.1. Nonconsensual Physical Searches Within the United States

C7.3.1.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes. The counterintelligence elements of the Military Departments are authorized to conduct nonconsensual physical searches in the United States for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.1.2., below.

C7.3.1.2. Other Nonconsensual Physical Searches. Except as permitted by section C7.1., above, DoD intelligence components may not conduct nonconsensual physical searches of persons and property within the United States for foreign intelligence or counterintelligence purposes. DoD intelligence components may, however, request the FBI to conduct such searches. All such requests, shall be in writing; shall contain the information required in subparagraphs C7.3.2.2.1., through C7.3.2.2.2.6., below; and be approved by an official designated in subparagraph C7.3.2.2.2.3., below. A copy of each such request shall be furnished the General Counsel, DoD.

C7.3.2. Nonconsensual Physical Searches Outside the United States

C7.3.2.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes. The counterintelligence elements of the Military Departments may conduct nonconsensual physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.2.2.2., below.

C7.3.2.2. Other Nonconsensual Physical Searches. DoD intelligence components may conduct other nonconsensual physical searches for foreign intelligence and counterintelligence purposes of the person or property of United States persons outside the United States only pursuant to the approval of the Attorney General. Requests for such approval will be forwarded by a senior official designated in subparagraph C7.3.2.3., below, to the Attorney General and shall include:

C7.3.2.2.1. An identification of the person or description of the property to be searched.

C7.3.2.2.2. A statement of facts supporting a finding that there is probable cause to believe the subject of the search is:

C7.3.2.2.2.1. A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities;

C7.3.2.2.2.2. A person who is an officer or employee of a foreign power;

C7.3.2.2.2.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power does not justify a nonconsensual physical search without evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C7.3.2.2.2.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C7.3.2.2.2.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

C7.3.2.2.3. A statement of facts supporting a finding that the search is necessary to obtain significant foreign intelligence or counterintelligence.

C7.3.2.2.4. A statement of facts supporting a finding that the significant foreign intelligence or counterintelligence expected to be obtained could not be obtained by less intrusive means.

C7.3.2.2.5. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search.

C7.3.2.2.6. A description of the extent of the search and a statement of facts supporting a finding that the search will involve the least amount of physical intrusion that will accomplish the objective sought.

C7.3.2.2.7. A description of the expected dissemination of the product of the search, including a description of the procedures that will govern the retention and dissemination of information about United States persons acquired incidental to the search.

C7.3.2.3. Requests for approval of nonconsensual physical searches under subparagraph C7.3.2.2., must be made by:

C7.3.2.3.1. The Secretary or the Deputy Secretary of Defense;

C7.3.2.3.2. The Secretary or the Under Secretary of a Military Department;

C7.3.2.3.3. The Director, National Security Agency; or

C7.3.2.3.4. The Director, Defense Intelligence Agency.

## C8. CHAPTER 8

### PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

#### C8.1. APPLICABILITY

This procedure applies to the opening of mail in United States postal channels, and the use of mail covers with respect to such mail, for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from United States persons where such activity is conducted outside the United States and such mail is not in United States postal channels.

#### C8.2. EXPLANATION OF UNDEFINED TERMS

##### C8.2.1. Mail Within United States Postal Channels includes:

C8.2.1.1. Mail while in transit within, among, and between the United States, its territories and possessions (including mail of foreign origin that is passed by a foreign postal administration, to the United States Postal Service for forwarding to a foreign postal administration under a postal treaty or convention, and mail temporarily in the hands of the United States Customs Service or the Department of Agriculture), Army-Air Force (APO) and Navy (FPO) post offices, and mail for delivery to the United Nations, NY; and

C8.2.1.2. International mail enroute to an addressee in the United States or its possessions after passage to United States Postal Service from a foreign postal administration or enroute to an addressee abroad before passage to a foreign postal administration. As a rule, mail shall be considered in such postal channels until the moment it is delivered manually in the United States to the specific addressee named on the envelope, or his authorized agent.

##### C8.2.2. To examine mail means to employ a mail cover with respect to such mail.

C8.2.3. Mail cover means the process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service.

### C8.3. PROCEDURES

#### C8.3.1. Searches of Mail Within United States Postal Channels

C8.3.1.1. Applicable postal regulations do not permit DoD intelligence components to detain or open first-class mail within United States postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service.

C8.3.1.2. DoD intelligence components may request appropriate U.S. postal authorities to inspect, or authorize the inspection, of the contents of second-, third-, or fourth-class mail in United States postal channels, for such purposes, in accordance with applicable postal regulations. Such components may also request appropriate U.S. postal authorities to detain, or permit the detention of, mail that may become subject to search under this section, in accordance with applicable postal regulations.

#### C8.3.2. Searches of Mail Outside United States Postal Channels

C8.3.2.1. DoD intelligence components are authorized to open mail to or from a United States person that is found outside United States postal channels only pursuant to the approval of the Attorney General. Requests for such approval shall be treated as a request for a nonconsensual physical search under subparagraph C7.3.2.2., of Procedure 7.

C8.3.2.2. Heads of DoD intelligence components may authorize the opening of mail outside U.S. postal channels when both the sender and intended recipient are other than United States persons if such searches are otherwise lawful and consistent with any Status of Forces Agreement that may be in effect.

#### C8.3.3. Mail Covers

C8.3.3.1. DoD intelligence components may request U.S. postal authorities to examine mail in U.S. postal channels, for counterintelligence purposes, in accordance with applicable postal regulations.

C8.3.3.2. DoD intelligence components may also request mail covers with respect to mail to or from a United States person that is outside U.S. postal channels, in accordance with appropriate law and procedure of the host government, and any Status of Forces Agreement that may be effect.

## C9. CHAPTER 9

### PROCEDURE 9. PHYSICAL SURVEILLANCE

#### C9.1. APPLICABILITY

This procedure applies only to the physical surveillance of United States persons by DoD intelligence components for foreign intelligence and counterintelligence purposes. This procedure does not apply to physical surveillance conducted as part of a training exercise when the subjects are participants in the exercise.

#### C9.2. EXPLANATION OF UNDEFINED TERMS

The term physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance.

#### C9.3. PROCEDURES

C9.3.1. Criteria for Physical Surveillance In the United States. Within the United States, DoD Intelligence components may conduct nonconsensual physical surveillances for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence component concerned; present or former contractors of such components or their present or former employees; applicants for such employment or contracting; or military persons employed by a non-intelligence element of a Military Service. Any physical surveillance within the United States that occurs outside a DoD installation shall be coordinated with the FBI and other law enforcement agencies, as may be appropriate.

C9.3.2. Criteria for Physical Surveillance Outside the United States. Outside the United States, DoD Intelligence components may conduct nonconsensual physical surveillance of United States persons in one of the categories identified in paragraph C9.3.1., above. In addition, such components may conduct physical surveillance of other United States persons in the course of a lawful foreign intelligence or counterintelligence investigation, provided:

C9.3.2.1. Such surveillance is consistent with the laws and policy of the host government and does not violate any Status of Forces Agreement that may be in effect;

C9.3.2.2. That physical surveillance of a United States person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot be obtained by other means.

C9.3.3. Required Approvals for Physical Surveillance

C9.3.3.1. Persons Within DoD Investigative Jurisdiction. Physical surveillances within the United States or that involve United States persons within DoD investigative jurisdiction overseas may be approved by the head of the DoD intelligence component concerned or by designated senior officials of such components in accordance with this procedure.

C9.3.3.2. Persons Outside DoD Investigative Jurisdiction. Outside the United States, physical surveillances of United States persons who are not within the investigative jurisdiction of the DoD intelligence component concerned will be forwarded through appropriate channels to the Deputy Under Secretary of Defense (Policy) for approval. Such requests shall indicate coordination with the Central Intelligence Agency.



## C10. CHAPTER 10

### PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

#### C10.1. APPLICABILITY

This procedure applies to participation by employees of DoD intelligence components in any organization within the United States, or any organization outside the United States that constitutes a United States person, when such participation is on behalf of any entity of the intelligence community. These procedures do not apply to participation in organizations for solely personal purposes.

#### C10.2. EXPLANATION OF UNDEFINED TERMS

C10.2.1. Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization or person.

C10.2.2. The term organization includes corporations and other commercial organizations, academic institutions, clubs, professional societies, associations, and any other group whose existence is formalized in some manner or otherwise functions on a continuing basis.

C10.2.3. An organization within the United States means all organizations physically located within the geographical boundaries of the United States whether or not they constitute a United States persons. Thus, a branch, subsidiary, or office of an organization within the United States, which is physically located outside the United States, is not considered as an organization within the United States.

C10.2.4. Participation refers to any action undertaken within the structure or framework of the organization involved. Such actions include serving as a representative or agent of the organization; acquiring membership; attending meetings not open to the public, including social functions for the organization as a whole; carrying out the work or functions of the organization; and contributing funds to the organization other than in payment for goods or services. Actions taken outside the organizational framework, however, do not constitute participation. Thus, attendance at meetings or social gatherings that involve organization members, but are not functions or activities of the organization itself does not constitute participation.

C10.2.5. Participation is on behalf of an agency within the intelligence community when an employee is tasked or requested to take action within an organization for the benefit of such agency. Such employee may already be a member of the organization or may be asked to join. Actions undertaken for the benefit of an intelligence agency include collecting information, identifying potential sources or contacts, or establishing and maintaining cover. If a cooperating source furnishes information to an intelligence agency that he or she obtained by participation within an organization, but was not given prior direction or tasking by the intelligence agency to collect such information, then such participation was not on behalf of such agency.

C10.2.6. Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit.

### C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION

Except as permitted herein, employees of DoD intelligence components may participate on behalf of such components in organizations within the United States, or in organizations outside the United States that constitute United States persons, only if their affiliation with the intelligence component concerned is disclosed to an appropriate official of the organization in accordance with section C10.4., below. Participation without such disclosure is permitted only if it is consistent with the limitations set forth in paragraph C10.3.1., below, and has been approved in accordance with paragraph C10.3.2., below.

#### C10.3.1. Limitations On Undisclosed Participation

C10.3.1.1. Lawful Purpose. No undisclosed participation shall be permitted under this procedure unless it is essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of the collecting DoD intelligence component.

C10.3.1.2. Limitations On Use of Undisclosed Participation for Foreign Intelligence Purposes Within the United States. Undisclosed participation may not be authorized within the United States for the purpose of collecting foreign intelligence from or about a United States person, nor to collect information necessary to assess United States persons as potential sources of assistance to foreign intelligence activities. This does not preclude the collection of information about such persons, volunteered by cooperating sources participating in organizations to which such persons belong, however, if otherwise permitted by Procedure 2.

C10.3.1.3. Duration of Participation. Authorization to participate under subparagraphs C10.3.2.1., and C10.3.2.2., shall be limited to the period covered by such participation, which shall be no longer than 12 months. Participation that lasts longer than 12 months shall be re-approved by the appropriate official on an annual basis in accordance with this procedure.

C10.3.1.4. Participation for the Purpose of Influencing the Activities of the Organization or Its Members. No participation under this procedure shall be authorized for the purpose of influencing the activities of the organization in question, or its members, unless such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power. Any DoD intelligence component that desires to undertake participation for such purpose shall forward its request to the Deputy Under Secretary of Defense (Policy) setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity. Such participation may be approved by the DUSD(P) with the concurrence of the General Counsel, DoD.

#### C10.3.2. Required Approvals

C10.3.2.1. Undisclosed Participation That May Be Approved Within the DoD Intelligence Component. Undisclosed participation on behalf of a DoD intelligence component may be authorized with such component under the following circumstances:

C10.3.2.1.1. Participation in meetings open to the public. For purposes of this section, a seminar or conference sponsored by a professional organization that is open to persons of a particular profession, whether or not they are members of the organization itself or have received a special invitation, shall be considered a meeting open to the public.

C10.3.2.1.2. Participation in organizations that permit other persons acknowledged to the organization to be employees of the U.S. Government to participate.

C10.3.2.1.3. Participation in educational or professional organizations for the purpose of enhancing the professional skills, knowledge, or capabilities of employees.

C10.3.2.1.4. Participation in seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar types of meetings, sponsored by organizations in which the employee is a member, has been invited to participate, or

when the sponsoring organization does not require disclosure of the participants' employment affiliations, for the purpose of collecting significant foreign intelligence that is generally made available to participants at such meetings, and does not involve the domestic activities of the organization or its members.

C10.3.2.2. Participation That May Be Approved By Senior Intelligence Officials. Undisclosed participation may be authorized by the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Commanding General, U.S. Army Intelligence and Security Command; the Director of Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, United States Air Force; the Director, Naval Investigative Service; the Commanding Officer, Air Force Office of Special Investigations; or their single designees, for the following purposes:

C10.3.2.2.1. To collect significant foreign intelligence outside the United States, or from or about other than United States persons within the United States, provided no information involving the domestic activities of the organization or its members may be collected.

C10.3.2.2.2. For counterintelligence purposes, at the written request of the Federal Bureau of Investigation.

C10.3.2.2.3. To collect significant counterintelligence about other than United States persons, or about United States persons who are within the investigative jurisdiction of the Department of Defense, provided any such participation that occurs within the United States shall be coordinated with the Federal Bureau of Investigation.

C10.3.2.2.4. To collect information necessary to identify and assess other than United States persons as potential sources of assistance for foreign intelligence and counterintelligence activities.

C10.3.2.2.5. To collect information necessary to identify United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

C10.3.2.2.6. To develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities.

C10.3.2.2.7. Outside the United States, to assess United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

#### C10.4. DISCLOSURE REQUIREMENT

C10.4.1. Disclosure of the intelligence affiliation of an employee of a DoD intelligence component shall be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization concerned.

C10.4.2. Disclosure may be made by the DoD intelligence component involved, an authorized DoD official, or by another component of the Intelligence Community that is otherwise authorized to take such action on behalf of the DoD intelligence component concerned.

## C11. CHAPTER 11

### PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES

#### C11.1. APPLICABILITY

This procedure applies to contracting or other arrangements with United States persons for the procurement of goods and services by DoD intelligence components within the United States. This procedure does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. The latter situation is governed by Procedure 10.

#### C11.2. PROCEDURES

C11.2.1. Contracts with Academic Institutions. DoD intelligence components may enter into a contract for goods or services with an academic institution only if prior to the making of the contract, the intelligence component has disclosed to appropriate officials of the academic institution the fact of sponsorship by a DoD intelligence component.

C11.2.2. Contracts with Commercial Organizations, Private Institutions, and Individuals. Contracting by or for a DoD intelligence component with commercial organizations, private institutions, or private individuals within the United States may be done without revealing the sponsorship of the intelligence component if:

C11.2.2.1. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities; or

C11.2.2.2. There is a written determination by the Secretary or the Under Secretary of a Military Department, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, or the Deputy Under Secretary of Defense (Policy) that the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned.

C11.3. EFFECT OF NONCOMPLIANCE

No contract shall be void or voidable for failure to comply with this procedure.

## C12. CHAPTER 12

### PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES

#### C12.1. APPLICABILITY

This procedure applies to the provision of assistance by DoD intelligence components to law enforcement authorities. It incorporates the specific limitations on such assistance contained in E.O. 12333 (reference (a)), together with the general limitations and approval requirements of DoD Directive 5525.5 (reference (i)).

#### C12.2. PROCEDURES

C12.2.1. Cooperation with Law Enforcement Authorities. Consistent with the limitations contained in DoD Directive 5525.5 (reference (i)), and paragraph C12.2.2., below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:

C12.2.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

C12.2.1.2. Protecting DoD employees, information, property, and facilities;  
and

C12.2.1.3. Preventing, detecting, or investigating other violations of law.

C12.2.2. Types of Permissible Assistance. DoD intelligence components may provide the following types of assistance to law enforcement authorities:

C12.2.2.1. Incidentally acquired information reasonably believed to indicate a violation of Federal law shall be provided in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a));

C12.2.2.2. Incidentally acquired information reasonably believed to indicate a violation of State, local, or foreign law may be provided in accordance with procedures adopted by the Heads of DoD Components;

C12.2.2.3. Specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law



enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to, Enclosure 3 of DoD Directive 5525.5 (reference (i)); and

C12.2.2.4. Personnel who are employees of DoD intelligence components may be assigned to assist Federal law enforcement authorities, and, when lives are endangered, State and local law enforcement authorities, provided such use is consistent with, and has been approved by an official authorized pursuant to, Enclosure 4 of DoD Directive 5525.5 (reference (i)). Such official shall ensure that the General Counsel of the providing DoD Component concurs in such use.

C12.2.2.5. Assistance may be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policy and applicable Status of Forces Agreements; provided, that DoD intelligence components may not request or participate in activities of such agencies undertaken against United States persons that would not be permitted such components under these procedures.

### C13. CHAPTER 13

#### PROCEDURE 13. EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

##### C13.1. APPLICABILITY

This procedure applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a DoD intelligence component. This procedure does not apply to experimentation on animal subjects.

##### C13.2. EXPLANATION OF UNDEFINED TERMS

C13.2.1. Experimentation in this context means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.

C13.2.2. Experimentation is conducted on behalf of a DoD intelligence component if it is conducted under contract to that component or to another DoD Component for the benefit of the intelligence component or at the request of such a component regardless of the existence of a contractual relationship.

C13.2.3. Human subjects in this context includes any person whether or not such person is a United States person.

##### C13.3. PROCEDURES

C13.3.1. Experimentation on human subjects conducted by or on behalf of a DoD intelligence component may be undertaken only with the informed consent of the subject, in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects.

C13.3.2. DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the Secretary or Deputy Secretary of Defense, or the Secretary or Under Secretary of a Military Department, as appropriate.

## C14. CHAPTER 14

### PROCEDURE 14. EMPLOYEE CONDUCT

#### C14.1. APPLICABILITY

This procedure sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this Regulation and other applicable policy. It also provides that DoD intelligence components shall ensure, as appropriate, that these policies and guidelines are made known to their employees.

#### C14.2. PROCEDURES

C14.2.1. Employee Responsibilities. Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by law; Executive order, including E.O. 12333 (reference (a)), and applicable DoD Directives.

##### C14.2.2. Familiarity With Restrictions

C14.2.2.1. Each DoD intelligence component shall familiarize its personnel with the provisions of E.O. 12333 (reference (a)), this Regulation, and any instructions implementing this Regulation that apply to the operations and activities of such component. At a minimum, such familiarization shall contain:

C14.2.2.1.1. Applicable portions of Procedures 1 through 4;

C14.2.2.1.2. A summary of other procedures that pertains to collection techniques that are, or may be, employed by the DoD intelligence component concerned; and

C14.2.2.1.3. A statement of individual employee reporting responsibility under Procedure 15.

C14.2.2.2. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IQ)) and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect that will achieve the objectives set forth in subparagraph C14.2.2.1., above.

C14.2.3. Responsibilities of the Heads of DoD Components. The Heads of DoD Components that constitute, or contain, DoD intelligence components shall:

C14.2.3.1. Ensure that all proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to applicable Executive Branch or DoD policy are referred to the General Counsel responsible for such component.

C14.2.3.2. Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15.

C14.2.3.3. Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder.

C14.2.3.4. In any case involving serious or continuing breaches of security by either DoD or non-DoD employees, recommend to the Secretary of Defense appropriate investigative actions.

C14.2.3.5. Ensure that the General Counsel and Inspector General with responsibility for the component, as well as the General Counsel, DoD, and the ATSD(IO), have access to all information concerning the intelligence activities of that component necessary to perform their oversight responsibilities.

C14.2.3.6. Ensure that employees cooperate fully with the Intelligence Oversight Board and its representatives.

## C15. CHAPTER 15

### PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE ACTIVITIES

#### C15.1. APPLICABILITY

This procedure provides for the identification, investigation, and reporting of questionable intelligence activities.

#### C15.2. EXPLANATION OF UNDEFINED TERMS

C15.2.1. The term "questionable activity," as used herein, refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive order or Presidential directive, including E.O. 12333 (reference (a)), or applicable DoD policy, including this Regulation.

C15.2.2. The terms "General Counsel" and "Inspector General," as used herein, refer, unless otherwise specified, to any General Counsel or Inspector General with responsibility for one or more DoD intelligence components. Unless otherwise indicated, the term "Inspector General" shall also include the ATSD(IO).

#### C15.3. PROCEDURES

##### C15.3.1. Identification

C15.3.1.1. Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO).

C15.3.1.2. Inspectors General, as part of their inspection of DoD intelligence components, and General Counsels, as part of their oversight responsibilities shall seek to determine if such components are involved in any questionable activities. If such activities have been or are being undertaken, the matter shall be investigated under paragraph C15.3.2., below. If such activities have been undertaken, but were not reported, the Inspector General shall also ascertain the reason for such failure and recommend appropriate corrective action.

C15.3.1.3. Inspectors General, as part of their oversight responsibilities, shall, as appropriate, ascertain whether any organizations, staffs, or offices within their respective jurisdictions, but not otherwise specifically identified as DoD intelligence components, are being used for foreign intelligence or counterintelligence purposes to which Part 2 of E.O. 12333 (reference (a)), applies, and, if so, shall ensure the activities of such components are in compliance with this Regulation and applicable DoD policy.

C15.3.1.4. Inspectors General, as part of their inspection of DoD intelligence components, shall ensure that procedures exist within such components for the reporting of questionable activities, and that employees of such components are aware of their responsibilities to report such activities.

#### C15.3.2. Investigation

C15.3.2.1. Each report of a questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy.

C15.3.2.2. When appropriate, questionable activities reported to a General Counsel shall be referred to the corresponding Inspector General for investigation, and if reported to an Inspector General, shall be referred to the corresponding General Counsel to determine whether the activity is legal and consistent with applicable policy. Reports made to the DoD General Counsel or the ATSD(IO) may be referred, after consultation between these officials, to the appropriate Inspector General and General Counsel for investigation and evaluation.

C15.3.2.3. Investigations shall be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from within the component concerned, or from other DoD Components, when necessary, to complete such investigations in a timely manner.

C15.3.2.4. To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation.

#### C15.3.3. Reports

C15.3.3.1. Each General Counsel and Inspector General shall report immediately to the General Counsel, DoD, and the ATSD(IO) questionable activities of a serious nature.

C15.3.3.2. Each General Counsel and Inspector General shall submit to the ATSD(IO) a quarterly report describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive order or Presidential directive, or applicable DoD policy; and actions taken with respect to such activities. The reports shall also include significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system. Separate, joint, or consolidated reports may be submitted. These reports should be prepared in accordance with DoD Directive 5000.11 (reference (j)).

C15.3.3.3. All reports made pursuant to subparagraphs C15.3.3.1., and C15.3.3.2., above, which involve a possible violation of Federal criminal law shall be considered by the General Counsel concerned in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a)).

C15.3.3.4. The General Counsel, DoD, and the ATSD(IO) may review the findings of other General Counsels and Inspectors General with respect to questionable activities.

C15.3.3.5. The ATSD(IO) and the General Counsel, DoD, shall report in a timely manner to the White House Intelligence Oversight Board all activities that come to their attention that are reasonably believed to be illegal or contrary to Executive order or Presidential directive. They will also advise appropriate officials of the Office of the Secretary of Defense of such activities.

C15.3.3.6. These reporting requirements are exempt from format approval and licensing in accordance with paragraph VII.G. of Enclosure 3 to DoD Directive 5000.19 (reference (k)).





INTELLIGENCE

UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

OCT 24 2005

MEMORANDUM FOR DEPUTY CHIEF OF STAFF, G-2, DEPARTMENT OF  
THE ARMY  
GENERAL COUNSEL, DEPARTMENT OF THE  
NAVY  
SECRETARY OF THE AIR FORCE, INSPECTOR  
GENERAL, DEPARTMENT OF THE AIR FORCE  
DIRECTOR, DEFENSE INTELLIGENCE AGENCY  
DIRECTOR, DEFENSE THREAT REDUCTION  
AGENCY  
DIRECTOR, MISSILE DEFENSE AGENCY  
DIRECTOR, NATIONAL GEOSPATIAL-  
INTELLIGENCE AGENCY  
DIRECTOR, NATIONAL SECURITY AGENCY  
DIRECTOR, NATIONAL RECONNAISSANCE  
OFFICE  
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Mission Tasking Authority

The demands on the Department of Defense (DoD) Counterintelligence (CI) have never been greater or more important. We must continue the transformation of our CI program to ensure a global capability that provides military commanders and other Department consumers and our national leadership with a horizontally integrated CI program that is responsive to the threats of today and the future. Our CI must be agile, integrated, comprehensive, proactive and responsive.

The Department created the Counterintelligence Field Activity (CIFA) to lead the transformation of our CI program, and the results have been impressive. The maturation of CIFA and the need for a more centralized approach to some of our key CI programs mandate additional authorities for CIFA. The Weapons of Mass Destruction Commission recently noted a need for CIFA to have an expanded role in the Department, and I concur.

Effective immediately, the Director, CIFA, will have the authority to task a Military Department CI organization or a Defense Agency's organic CI element to execute a specific CI mission or conduct a CI function within that organization's



charter. Should a question arise about such a tasking that cannot be resolved, it should be referred to the Deputy Under Secretary of Defense (Counterintelligence and Security) via the Counterintelligence Directorate. The point of contact is Mr. Troy Sullivan, Director, Counterintelligence ((703) 697-7641 ext. 350). This authority will be incorporated into DoDD 5240.2, DoD Counterintelligence, which is currently being revised.

I appreciate your support in this most important area.



Stephen A Cambone

cc:

Director, Counterintelligence Field Activity



OFFICE OF THE UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

DEC 01 2005

MEMORANDUM FOR PUBLIC RELEASE

FROM DUSD (CI&S)

SUBJECT: BACKGROUND PAPER, DEPARTMENT OF DEFENSE  
COUNTERINTELLIGENCE FIELD ACTIVITY

The Counterintelligence Field Activity (CIFA) was established on February 19, 2002, and charged with developing and managing Department of Defense (DoD) Counterintelligence (CI) programs and functions that support the protection of the Department. This includes CI support to protect its personnel, resources, critical information, research and development programs, critical infrastructure, economic security, and U.S. interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against the Department.

CIFA's origins can be traced to Presidential Decision Directive 75, signed by President Clinton on January 5, 2001, and subsequently revalidated by the Bush Administration. PDD-75 called for a predictive and proactive CI system with integrated oversight of CI issues across the national security agencies. Within DoD, CIFA was identified as the Department's single coordination focal point for CI policy implementation, and Defense-wide CI resource and budget planning.

Within DoD, the Military Departments, not CIFA, are charged with the "full spectrum of CI functions." These include investigations and operations. CIFA is responsible for oversight of the CI activities of the Military Departments. The Silberman/Robb WMD Commission recommended CIFA be given authority to provide "full spectrum" CI support to these Components.

In consultation with the NSC staff charged with implementation of the WMD Commission's recommendation, DoD deferred granting CIFA "full spectrum" authorities. Instead, CIFA has been given Mission Tasking Authority (MTA). This new authority enhances CIFA's ability to coordinate the activities of the Military Department CI components to ensure that both Service and DoD-wide CI needs are met.



 **COPY**

The MTA in no way expands Departmental authorities nor does the MTA modify existing law or Department directives on the collection or retention of information about US persons. The MTA allows CIFA to task Department CI organizations to execute a specific mission or conduct a function falling within that organization's charter. This new authority is provided in the attached USD(I) Memorandum dated October 24, 2005. This memorandum and its attachment are cleared for public release.



Robert W. Rogalski  
Acting Deputy Under Secretary of Defense  
(Counterintelligence and Security)

Attachment:  
Mission Tasking Authority



UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

DEC 19 2005

The Honorable John W. Warner  
Chairman  
Committee on Armed Services  
United States Senate  
Washington, DC 20510-6050

Dear Mr. Chairman:

An NBC Nightly News segment aired on December 13th alleging that Department of Defense (DoD) entities are collecting information on American peace activists and monitoring protests against the Iraq war. The segment highlighted entries in the Department's Threat and Local Observation Notice (TALON) reporting system. I want to provide you some context not otherwise reported in the segment.

The Department is authorized to conduct an integrated and cooperative counterintelligence (CI) and military law enforcement effort that protects its installations, property and people from threats of all kinds – both overseas and in the United States. In support of this effort, designated DoD organizations report unfiltered information provided by concerned citizens, DoD personnel charged with responsibilities for the security of DoD installations (e.g., gate guards) or other DoD personnel reporting suspicious activities. That information is merged with information from local, state and federal law enforcement and other intelligence, security and CI organizations and is used by analysts to assess potential threats to DoD interests.

TALON is the place where DoD initially stores "dots" of information which if validated, might later be connected to avert an attack before it occurs. Under existing procedures, a "dot" of information that is not validated as threatening must be removed from the TALON system in less than 90 days. If the "dot" is validated, the information is transferred to law enforcement.

I have directed that the appropriate CI and military law enforcement organizations within the Department take several actions. A thorough review of the TALON reporting system is underway to ensure full compliance with DoD



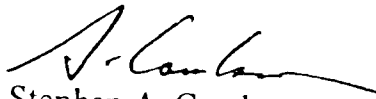
directives and U.S. laws. We will review those policies and procedures for proper application with respect to receipt and retention of information about U.S. persons. Finally, we will review the TALON database to determine whether information has been improperly used or stored in the database.

I have directed that all Department CI and intelligence personnel receive immediate refresher training concerning the laws, policies and procedures that govern the responsibilities for handling information, especially information related to U.S. persons.

My office is currently engaged in both formal and informal dialogue with members of your staff on this subject. We stand ready to answer questions you may have.

I have sent a similar letter to the Committee's Ranking Member, the Honorable Carl Levin.

Sincerely,



Stephen A. Cambone



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

JAN 13 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Retention and Use of Information for the TALON System

The TALON reporting program was initiated in May 2003 to provide a mechanism for reporting and analyzing non-validated possible terrorist-related threat information. This initiative provides the Department with a system to permit a comprehensive analysis of potential terrorist-related threats. This program has been designed with respect for the civil liberties of our fellow citizens. Accordingly, with respect to the TALON program, I direct the following.

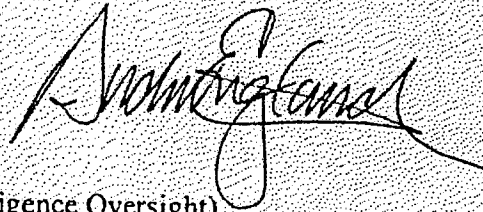
- All DoD intelligence and counterintelligence (CI) personnel will receive refresher training on the policies for collection, retention, dissemination and use of information related to U.S. Persons. The refresher training is to be completed by January 31, 2006. Components will notify USD(I) when that training is complete.
- The Director, Counterintelligence Field Activity will advise Under Secretary of Defense for Intelligence (USD(I)) by January 17, 2006, that all reports in the TALON database have been reviewed to identify any reports that should not be in the database.

The USD(I) has chartered a working group to review and recommend changes to policy and procedures employed in the TALON program to ensure compliance with DoD policy. The USD(I) will provide recommendations to me no later than February 15, 2006.

OSD 00536-06



Any questions concerning this guidance may be directed to Mr. [REDACTED]  
OUSD(I), CI, Directorate, [REDACTED] Ext- [REDACTED] NIPR: [REDACTED]  
SIPR: [REDACTED] Components will notify Mr. [REDACTED]  
when refresher training is completed.



cc:  
Assistant to the Secretary of Defense (Intelligence Oversight)





OFFICE OF THE UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

JAN 27 2006

The Honorable John W. Warner  
Chairman  
Committee on Armed Services  
United States Senate  
Washington, DC 20510-6050

Dear Mr. Chairman:

In the Under Secretary of Defense for Intelligence letter of December 19, 2005, Dr. Stephen Cambone provided you some context not otherwise reported in an NBC News segment on the Department of Defense (DoD) TALON system. Dr. Cambone also advised that we would thoroughly review the TALON system. That review is nearly completed. I would like to update you on our results:

- DoD field commanders highly value the TALON reporting program as a source of timely information about possible foreign terrorist threats to their personnel and facilities.

The TALON reporting system is much like a capability to document information from a "neighborhood watch" program in which concerned citizens or DoD personnel report suspicious activities they believe may be linked to possible foreign terrorist activities to DoD counterintelligence, law enforcement or intelligence organizations. The focus of the effort was on possible foreign terrorist threats to the DoD and not on U.S. persons in the United States. The information that was reported to DoD security, law enforcement, counterintelligence or intelligence personnel was then briefed to local military command officials and law enforcement as appropriate prior to being sent to the TALON reporting database at the Counterintelligence Field Activity (CIFA) for analysis. CIFA's role in the process is to maintain the database and conduct analysis.

- TALON reporting has led to a number of investigations. Those include terrorism investigations, most often conducted under the purview of the Joint Terrorism Task Forces headed by FBI, and the reporting has identified other criminal activities. The reporting has also disclosed



some patterns that have allowed the Department to focus or change security procedures in order to deter potential terrorist activities.

- Although the TALON reporting system was intended to document suspicious incidents possibly linked to foreign terrorist threats to DoD resources, some came to view the system as a means to report information about demonstrations and anti-base activity that would be of interest to field commanders from a force protection perspective. A very small percentage of these reports were submitted to the TALON/CORNERSTONE database.
- CIFA has removed the TALON reports on demonstrations and anti-base activity from the database. The process to remove other reports that are no longer analytically significant is ongoing. All TALON reports are now reviewed at CIFA upon receipt to ensure compliance with the TALON reporting criteria.
- The DoD organizations involved in the TALON reporting system were following multiple rule sets regarding the collection and retention of this information. The Department will soon issue detailed guidance that clarifies the purpose of the database, the rules governing the collection and retention of the data and more detailed procedures to be followed. The database will then be reviewed again to ensure compliance.

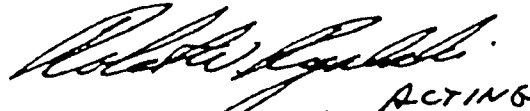
Dr. Cambone also directed that all Department counterintelligence and intelligence personnel receive immediate refresher training concerning the laws, policies and procedures that govern the responsibilities for handling information, especially information related to U.S. persons. The refresher training is underway and should be completed by January 31, 2006.

This review clearly indicates that TALON is an important and valuable tool, and that we have room for improvement. We will continue our analysis of findings from this review to determine precisely what we need to do to improve and will provide you with additional information.

There is nothing more important to the U.S. military than the trust and good will of the American people. The DoD values that trust and good will and consequently views with the greatest concern any potential violation of the strict DoD policy governing the protection of civil liberties. Our new guidance will reflect that concern and protect that trust.

My office continues to be engaged in formal and informal dialogue with members of your staff on this subject. These discussions have been positive and productive. I look forward to an opportunity to brief your committee on these complex and overlapping issues. I have sent a similar letter to the Committee's Ranking Member, the Honorable Carl Levin.

Sincerely,

A handwritten signature in dark ink, appearing to read "Robert W. Rogalski".

Robert W. Rogalski *ACTING*  
Deputy Under Secretary of Defense  
(Counterintelligence and Security)

cc:

The Honorable Ted Stevens  
The Honorable Daniel K. Inouye  
The Honorable C.W. "Bill" Young  
The Honorable John P. Murtha  
The Honorable Duncan Hunter  
The Honorable Ike Skelton  
The Honorable Pat Roberts  
The Honorable John D. Rockefeller IV  
The Honorable Peter Hoekstra  
The Honorable Jane Harman



INTELLIGENCE

UNDER SECRETARY OF DEFENSE

5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

FEB 2 2006

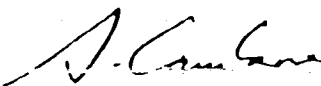
MEMORANDUM FOR DIRECTOR, COUNTERINTELLIGENCE  
FIELD ACTIVITY

SUBJECT: The TALON/CORNERSTONE Database

TALON reporting is an important capability in providing Department of Defense (DoD) analysts with unfiltered reports of possible terrorist activity that might otherwise be lost. The Counterintelligence Field Activity (CIFA) plays a key role in this program. As a result of the TALON reporting review that has been ongoing for several weeks, I believe a change is required in the policy CIFA uses to retain U.S. persons information in the TALON/CORNERSTONE database.

CIFA will ensure all TALON reporting maintained within the TALON/CORNERSTONE database, or elsewhere in CIFA, is maintained under procedures contained within DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982. The DoD Office of the General Counsel (OGC) provided you guidance regarding the application of this policy to the TALON/CORNERSTONE database. Please begin a review immediately to ensure all reports within the TALON/CORNERSTONE database are retained pursuant to DoD 5240.1-R, and in accordance with OGC guidance. Additionally, provide the Acting Deputy Undersecretary of Defense, Counterintelligence and Security, weekly status reports on the progress of your review.

Since the TALON/CORNERSTONE database is a counterintelligence database for possible foreign terrorist-related information, oversight for the TALON holdings within the database will fall to the office of the Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IO)). CIFA will work closely with the ATSD(IO) to ensure TALON information is appropriately maintained, employing to the fullest extent possible the authorities to retain foreign terrorist threat information for analysis.

  
Stephen A. Cambone

cc:  
ATSD(IO)  
OGC (Ms. Watson)





## DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
ASSISTANT TO THE SECRETARY OF  
DEFENSE FOR INTELLIGENCE OVERSIGHT  
GENERAL COUNSEL OF THE DEPARTMENT  
OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF  
DEFENSE  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Threats to the Department of Defense (DoD)

The TALON Reporting System is an innovative initiative to document unfiltered and non-validated potential threat information about suspicious activity linked to possible international terrorist threats to DoD personnel and resources that might have otherwise gone unreported. This information is reported by concerned citizens and Department personnel or obtained through information sharing with civilian law enforcement agencies. The program has been productive. It has detected international terrorist interest in specific military bases and has led to and supported counterterrorism investigations.

The Department has completed the review and assessment of the TALON Reporting System addressed in my memorandum of January 13, 2006, "Retention and Use of Information for the TALON System." This review confirmed that the TALON Reporting System should be used only to report information regarding possible international terrorist activity and concluded that all TALON reports should be retained in accordance with DoDD 5240.1-R, "Activities of DoD Intelligence Components That Affect United States Persons," dated December 1982.

To ensure the continued effectiveness of the TALON Reporting System, I am directing all DoD components that use the TALON Reporting System to comply with the procedures listed in Enclosure (1) and to ensure the information included in their TALON reports meet the criteria for reporting described in Enclosure (1).

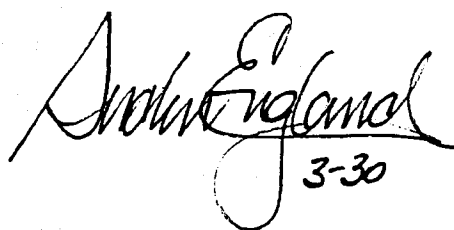
This Memorandum provides interim guidance. Given the importance of capturing threat information in protecting the Department's personnel, property and facilities, I am Directing the Under Secretary of Defense for Intelligence (USD(I)) to convene a working group to examine the integration of threat information across the DoD intelligence, counterintelligence, law enforcement, force protection and security communities. The



USD(I) will report the findings of this working group to me by Sep 15, 2006. The interim guidance contained in this memorandum will remain in effect until the above described working group's findings are published and permanent TALON Reporting System policy is promulgated.

By this memorandum I am also directing the Assistant to the Secretary of Defense (Intelligence Oversight), on an annual basis, to review the TALON Reporting System and to provide a report to the USD(I) with the status of the first review within 60 days. The USD(I) and the DoD Counterintelligence Field Activity (CIFA) will work with the DoD Inspector General on its ongoing audit of the TALON Reporting System.

The May 2, 2003, Deputy Secretary of Defense Memorandum, titled, "Collection, Reporting and Analysis of Terrorist Threats to DoD Within the United States," (Enclosure 2) required the identification of "lead components" within the Military Departments to distribute TALON reporting from their respective Departments. I hereby direct each lead component to provide to CIFA, by May 12, 2006, a copy of its guidance to implement the process set forth in Enclosure (1). CIFA will review each Department's guidance to insure it conforms with the process in Enclosure (1) and will provide a status report to the Deputy Under Secretary of Defense (Counterintelligence and Security) by May 30, 2006.



3-30

Enclosures:

1. TALON REPORTING SYSTEM PROCEDURES
2. Deputy Secretary of Defense memo of May 2, 2003, Subject: "Collection, Reporting and Analysis of Terrorist Threats to DoD Within the United States"

Enclosure (1) to Deputy Secretary of Defense Memorandum, "Threats to the Department of Defense"

## TALON REPORTING SYSTEM PROCEDURES

- The guidance for the TALON Reporting System as provided in Deputy Secretary of Defense Wolfowitz's memo of May 2, 2003, "Collection, Reporting and Analysis of Terrorist Threats to the Department of Defense (DoD) Within the United States," (Enclosure (2)) remains in force. This document updates and clarifies that guidance.
- The TALON Reporting System is the Department's mechanism to gather, share, compile, and retain unfiltered non-validated threat or suspicious activity information possibly linked to international terrorist activities posing a potential threat to DoD personnel and resources both domestically and abroad.

## REPORTING TALON INFORMATION

A proposed TALON report must meet one of the following seven criteria (the criteria remain substantially the same as in the DepSecDef memo of May 2, 2003):

1. Specific or non-specific threats to DoD interests.
  2. Suspected surveillance of DoD facilities or personnel.
  3. Elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests.
  4. Tests of security.
  5. Unusual repetitive activity.
  6. Bomb threats.
  7. Any other suspicious activity and incidents reasonably believed to be related to international terrorist activity directed against DoD personnel, property, and activities within the United States or abroad.
- An appropriate level supervisor in each DoD organization authorized to submit TALON reports shall review each proposed report prior to submission to the Counterintelligence Field Activity (CIFA) to ensure it meets one of the reporting criteria listed above and one of the following detailed criteria descriptions:

1. Specific or Non-Specific Threats: Specific threats are threats received by any means, which contain a time, location or area for an attack against US forces, facilities, or missions. Non-specific threats include, but are not limited to, any event or incident, or series of events or incidents, which in and of themselves may indicate the potential for a threat to US forces, facilities or mission, regardless of whether the threat posed is deliberately targeted or collateral.
  2. Surveillance: Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts may include use of cameras (either still or video), note taking, annotated maps or drawings, hand-drawn maps or diagrams, use of binoculars or other vision enhancing devices, or any reports from host nation security forces of possible surveillance of US assets.
  3. Elicitation: Any attempts to obtain security-related or military-specific information by anyone who does not have the appropriate security clearance and the need-to-know. Elicitation attempts may be made by mail, fax, telephone, by computer, or in person.
  4. Test of Security: Any attempts to measure security reaction times or strength; any attempts to test or penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, or other security related documents.
  5. Repetitive Activities: Any activities that meet one of the other TALON criteria and have occurred two or more times – the same activity by the same person and/or vehicle, within a one month period.
  6. Bomb Threats: Communication by means specifically threatening to use a bomb to attack US forces, facilities or missions.
  7. Suspicious Activities/Incidents: This category should only be used if the TALON information does not meet any of the above criteria. Any activity/incident that does not specifically fit into the aforementioned six categories yet is believed to represent a potential threat should be reported under this category. Examples of this include: an anomaly noticed resulting from the deployment of homeland defense assets; theft of material that could be used to manufacture false identification cards; thefts of military uniforms which may be used to gain access to military installation, etc.
- If information meets the reporting criteria set forth above, the reporting organization is deemed to hold a reasonable belief that there is a nexus between the information



and "international terrorist activity," and it may be forwarded to CIFA as a TALON report for inclusion in the Cornerstone database.

- If a TALON reporting entity determines that a TALON report is of interest to local command authorities, law enforcement (DoD and/or non-DoD) or homeland defense entities, it may share the information in the report with those organizations via established lines of communication.
- CIFA will conduct a review of all TALON reports submitted to the Cornerstone database to confirm they meet the reporting criteria. CIFA shall immediately remove from the database any report that does not meet the criteria. CIFA will notify the submitter of the TALON report of the removal and verify the reporting entity also purges the TALON report from its system.
- Credible information about a possible international terrorist threat sufficient to warrant an investigation must be referred to the proper investigative agency immediately by the reporter and/or CIFA.
- Information that is responsive to existent intelligence or counterintelligence DoD collection requirements must be reported in Intelligence Information Reports and not entered into the TALON Reporting System.

#### RETAINING TALON REPORTS

- Only DoD intelligence and counterintelligence organizations may retain TALON reports. DoDD 5240.1-R, "Activities of DoD Intelligence Components That Affect United States Persons," dated December 1982 governs the retention of US person information in TALON reports. Identifying US person information in TALON reports and in the Cornerstone database may be retained indefinitely if there is a reasonable belief the person is engaged in or about to engage in international terrorist activities. If this reasonable belief cannot be established within 90 days from the time the information is collected, the identifying US person information may not be retained by any intelligence or counterintelligence organization. CIFA will remove the US person information from the Cornerstone database and notify the submitting component of the removal. The submitting component must also remove the US person information from its system and advise CIFA of the removal within 5 days of receiving the notification from CIFA.
- However, the US person information may be disseminated by CIFA to a law enforcement entity prior to its removal from the Cornerstone database if the information is of interest to law enforcement and meets legal requirements for transfer of the information. Law enforcement organizations may request from CIFA, and

CIFA may provide to them, any TALON reports held for which the law enforcement organization has a legitimate legal requirement.

### ANALYSIS OF TALONS

- Any organization that identifies possible international terrorist activity based upon TALON Reporting System analysis will immediately notify the appropriate law enforcement agencies, command authorities and CIFA.
- Any organization that determines a previously submitted TALON report is not linked to possible international terrorist activity will immediately notify CIFA so that CIFA can remove the report from the Cornerstone Database. CIFA will notify TALON Reporting System users of the reports that it deletes from the Cornerstone database, based on its own analysis or that of any other organizations, and the users must notify CIFA within 5 days of receiving the notification that they have also deleted the report from their system(s). Within 5 days of receiving a notification from CIFA, the TALON reporting entity must also notify any command authorities, law enforcement or homeland defense entity that received the information from the reporter that the information is not linked to possible international terrorist activity.

### ADMINISTRATIVE MATTERS

- CIFA is responsible for the maintenance of the Cornerstone database that is the central DoD repository for TALON reports.
- CIFA will continue to ensure only authorized personnel and organizations have access to the TALON Reporting System and Cornerstone database.
- Although the TALON Reporting System is focused on DoD facilities, interests or personnel, should non-specific information be received about suspicious activities possibly linked to international terrorist actions against non-DoD personnel, activities or facilities, that information should be provided to the appropriate local authorities.

~~FOR OFFICIAL USE ONLY~~

HRS (UPR)



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010



May 2, 2003

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Collection, Reporting, and Analysis of Terrorist Threats to DoD Within The  
United States

The Secretary of Defense has repeatedly underscored that the nation's war on terrorism ranks among the Department's highest national security priorities. Much has been accomplished by DoD's intelligence, counterintelligence, law enforcement, and security components to counter the terrorist threat in the wake of September 11<sup>th</sup>, 2001, however, there is more to be done. While DoD has an established process to identify, report, and analyze information regarding foreign terrorist threats, we have no formal mechanism to collect and share non-validated domestic threat information between intelligence, counterintelligence, law enforcement and force protection entities and subject that information to careful analysis for indications of foreign terrorist activity.

A new reporting mechanism, the "TALON" report, has been established to provide a means to capture non-validated domestic threat information, flow that information to analysts, and incorporate it into the DoD terrorism threat warning process. A TALON report consists of raw information reported by concerned citizens and military members regarding suspicious incidents. Information in TALON reports is non-validated, may or may not be related to an actual threat, and by its very nature may be fragmented and incomplete. The purpose of the TALON report is to document and immediately disseminate potential threat information to DoD personnel, facilities, and resources. The TALON mechanism is not designed to take the place of DoD's formal intelligence reporting process.

Therefore, I hereby direct the implementation of policies and processes, as well as the utilization of resources necessary to identify, report, share, and analyze non-validated threat information in the United States through the use of the TALON system. Effective immediately, all DoD intelligence, counterintelligence, law enforcement, and security organizations that have the mission to collect force protection and threat information shall

U05646-03

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

identify, collect, and report the following categories of information, in accordance with existing policy and law, consistent with the TALON framework established by the Joint Staff Domestic Threat Working Group (see attachment): (1) non-specific threats to DoD interests; (2) suspected surveillance of DoD facilities and personnel; (3) elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests; (4) tests of security; (5) unusual repetitive activity; (6) bomb threats; and (7) any other suspicious activity and incidents reasonably believed to be related to terrorist activity directed against DoD personnel, property, and activities within the United States.

I hereby direct the Secretaries of the Military Departments, the Combatant Commanders, and Agency Directors to designate those components within their respective organizations that have the mission to collect and report this information and, further, to designate a single component within their respective organizations to assume the lead for distribution of this information. Once lead components are identified, they shall be identified to both the DoD Inspector General and the Assistant to the Secretary of Defense (Intelligence Oversight).

Upon identification of such information, lead components shall produce TALON reports and provide them to appropriate local military commanders and others responsible for installation security before the information is released outside the installation. Lead components that receive TALON reports shall ensure they are provided directly to the DoD Counterintelligence Field Activity (CIFA) and to other appropriate military commanders as secondary (info) recipients as necessary. CIFA will incorporate the information into a database repository and provide full database access to the Defense Intelligence Agency, Joint Intelligence Task Force-Combating Terrorism (JITF-CT) in order to support its terrorism warning mission. The CIFA and designated "lead components" in the Military Services, Combatant Commands, and Defense Agencies are authorized to retain TALON information as necessary to conduct their analysis missions. The Under Secretary of Defense, Intelligence (USD/I) is the designated overall lead official for this matter and will, therefore, validate the need of other DoD organizations for access to this information.

This policy remains in effect until superseded or until appropriate DoD policy on this subject is published or revised.



Attachment:  
As stated

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

**SUBJECT:** Attachment to DepSecDef Memo re: Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States

## **BACKGROUND**

The TALON system is designed to report anomalies, observations that are suspicious against the steady state context, and immediate indicators of potential threats to DoD personnel and/or resources. TALON reports are raw, non-validated information, which may or may not be related to an actual threat, and by their very nature, may be fragmented and incomplete. Information contained in TALON reporting is designed for use by Commanders at all levels that have force protection responsibilities and for analysts to use to help determine the aggregate terrorist threat to DoD people and resources.

TALON reports are of a tactical nature, with rapid reporting as the goal, and may be less refined than Intelligence Information Reports (IIRs). TALON reports are designed to capture raw threat data that does not meet IIR criteria. Critical to the reports is the proper documentation of the basic interrogatories (who – ALL PEOPLE INVOLVED, what, when, where, why, and how), the source's knowledge of these, and a clear definition of facts versus opinion (source's or reporter's).

TALON reports augment but are not designed to replace standard reporting mechanisms. IIRs, information files, operational files, and substantive investigations case files and associated reports are to be documented as directed by existing policies and directives.

As a general guide, to the maximum extent possible, TALON reports should be classified at the lowest possible level to ensure maximum distribution of the information. The use of the Law Enforcement Sensitive caveat and higher classifications should be kept to a minimum.

TALON information must be swiftly briefed locally to commanders and security officials so appropriate actions can be taken before this information is released outside the installation level. TALON reports are to be sent using automated information systems or via email attachment as a word document either on the NIPRnet for unclassified reports or on SIPRnet to respective Component Headquarters. Reports will be made as soon as possible after developing the information. Respective elements in designated Components will provide the TALON reports to the DoD Counterintelligence Field Activity (CIFA) as directed in the main policy memo of this attachment. The CIFA will ensure the JTF-CT has full access to the raw, non-validated information. Designated lead Service and Agency components will have access to the TALON database.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

## TALON REPORT GUIDE

FOR OFFICIAL USE ONLY

### TALON Report

CAUTION: TALONs are preliminary reports on ambiguous circumstances, and may contain incompletely evaluated information. TALONs are intended to alert commanders & staff to anomalies, potential terrorist indicators, or other FP issues.

1. **DATE**: (Date report is generated).
2. **LOCATION**: Location where the incident occurred.
3. **REPORTING UNIT**: Unit submitting the report.
4. **SEQUENCE NUMBER**: Your Component generated unique number.
5. **TALON CRITERIA**: Enter one of the following:
  - a. **Non-specific Threats**. Threats received by any means, which contain a specific time, location or area for an attack against US forces, facilities or missions. This includes, but is not limited to, any event or incident, or series of events or incidents, which in and of themselves may indicate the potential for a threat to US forces, facilities, or mission, regardless of whether the threat posed is deliberately targeted or collateral.
  - b. **Surveillance**. Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts may include use of cameras (either still or video), note taking, annotated maps or drawings, hand-drawn maps or diagrams, use of binoculars or other vision enhancing devices, or any reports from host nation security forces of possible surveillance of US assets.
  - c. **Elicitation**. Any attempts to obtain security-related or military-specific information by anyone who does not have the appropriate security clearance and the need-to-know. Elicitation attempts may be made by mail, fax, telephone, by computer, or in person.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

d. Tests Of Security. Any attempts to measure security reaction times or strengths; any attempts to test or to penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, passes, or other security related documents.

e. Repetitive Activities. Any activities that meet one of the other TALON criteria and have occurred two or more times – the same activity by the same person and/or vehicle, within a 1 month period.

f. Bomb Threats: Communication by any means specifically threatening to use a bomb to attack against US forces, facilities or missions.

g. Suspicious Activities/Incidents: This category should **ONLY** be used if the TALON information **DOES NOT** meet any of the above criteria. Any activity/incident that does not specifically fit into the aforementioned six categories yet is believed to represent a force protection threat should be reported under this category. Examples of this include: issue resulting in the scrambling of homeland defense assets; thefts of material that could be used to manufacture false identification cards; thefts of military uniforms which may be used to gain access to a military installation, etc.

6. RELEASABLE TO: Assign appropriate release information (REL to UK/CAN)

7. CLASSIFICATION: Assign appropriate classification (FOUO, SECRET)

8. CAVEAT: Assign appropriate caveat ((LES, NOFORN)

9. STATUS: Choose Open/Unresolved, Closed/Unresolved or Closed/Resolved.

10. ONE LINE TITLE: Short title identifying what the TALON is about (i.e. Surveillance at Andrews AFB).

11. SOURCE AND ASSESSMENT OF CREDIBILITY: Who provided the information, how credible is the source, and why do you assess the source that way? (i.e. Desk Sgt, 82 SFS, direct access to information reported).

12. DETAILS: Who, What, When, Where, Why, and How. The most critical part of the report for the reader. Obtain all possible identification details of suspect(s) or suspected incident for further follow-up (including license plates). Be specific about what source said and about what source did not know (avoid second guessing by higher echelons). Use memory tools to aid source in remembering details (mild interrogation). For example, one tool all Army personnel are trained in, down to the troop level, is SALUTE. Size (size of suspicious element - e.g. "2 people"); Activity (what was going on - e.g. "drove by guard gate slowly"); Location (where did it happen - e.g. "guard post 3"); Unit (identification of unit involved - e.g. "local contractor hired TCN"); Time (when

~~FOR OFFICIAL USE ONLY~~

did it happen - e.g. "20:00 hours, 2 January 20\_\_"); Equipment (what were they carrying, driving, etc. - e.g. "in 1990 white Caprice, with binoculars, writing notes on an aviator knee pad").

13. **COUNTRIES** What countries does the information in the TALON relate to.
14. **PERSONS BRIEFED LOCALLY**: Who was briefed locally, and when were they notified of the incident, (i.e.: Base Commander, 82 SFS/CC, Phoenix JTTF, etc).
15. **ACTIONS TAKEN**: What investigative steps have already been accomplished.
16. **ACTIONS PENDING**: What investigative steps are you involved in or do you have planned to bring the incident to closure (running license plate checks, interview another witness, etc.)
17. **SUMMARIZE TALON**: Two to three sentences giving the basic summary of what the TALON is about. This is not a regurgitation of the details but a simple summary – should not contain any specific information. (i.e. Unknown individual observed photographing front gate of Andrews AFB. When approached, he left and a license plate was recorded. The license plate was identified as being invalid so no further information could be obtained). The specifics should be in the detail section. This is the short summary that, along with the one line title, if posted to the face of the webpage can gain the readers attention.
18. **COMMENTS**: Any information the reporting unit wants to convey and maintain as internal organization comments. Fully identify information sources here.
19. **PERSONS INVOLVED**: Fill-in the blocks – SUBJECTS, WITNESSES, INCIDENTALS

FOR OFFICIAL USE ONLY

~~FOR OFFICIAL USE ONLY~~